REMARKS

Claims 13 - 31 are pending in the present application. No amendments have been proposed. Reconsideration of the claims is respectfully requested in view of the following discussion.

As to the Merits:

As to the merits of this case, the Examiner sets forth the following rejection:

claims 13 - 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Roberts (U.S. Patent No. 5008,935) in view of the publication paper by Michael Portz, title "On the Use of Interconnection Networks in Cryptography".

This rejection is respectfully traversed.

Independent claim 13 recites *in a device for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key, the combination with a modified "P" permutation in the "f" function.*

Independent claim 25 recites *in a device for performing the "f" function of the Data Encryption Standard (DES), the combination with a modified permutation means to produce a modified permutation replacing the fixed permutation "P" of the DES.*

Independent claim 27 recites *a method for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key, in combination with a modified "P" permutation in the "f" function, comprising the step of: replacing the "P" permutation in the "f" function by said modified permutation.*

For example, as shown in Figure 3 of the present invention, there are important benefits regarding the specific position of the modified P* permutation (136) which include the capability to be backward compatible with the standard DES and its modes (e.g. OFB, ECB) and all its variants such as triple DES as well as the immense number of individual cryptographic algorithms stemming from the variations in the modified P and how they are generated and when they are changed. Another advantage of the placement of the modified P in the present invention is that the fundamental security features of DES are retained and expanded upon by the tremendous variations created by the modified P permutation.

With regard to the primary reference of Roberts, the Examiner correctly acknowledges that, "Roberts does not expressly disclose the modified permutation "P is actually inside the "f function of the DES'." [1]

That is, as clearly shown in Fig. 1 of Roberts, while each block encryptor 1 encrypts 8 bytes of using the DES algorithm, the permuter 11 fails to use the DES algorithm and instead, merely takes the 256 byte output of the 32 block encryptors and permutes the 256 bytes in conformance with a second key. See column 1, lines 54 – 63 of Roberts. In other words, the permutation of Roberts is done after the primary encryption in the final step of his scheme.

In order to compensate for the above-noted drawbacks and deficiencies of the primary reference of Roberts, the Examiner relies on the teaching of the secondary reference of Portz.

However, Portz also fails to disclose or fairly suggest the claimed features regarding performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key, the combination with a modified "P" permutation in the "f" function.

That is, Portz's paper mentions the DES algorithm in the context of a cryptosystem that is a generator of permutations, 1.1 lines 2-3. Portz also states, as the examiner points out in page 308 reference 2.3 "Virtual Interconnection Networks lines 5-6, "Cryptosystems like DES & RSA

[1] Please see, page 3, lines 8-10 of the Action.

usually describe sets of permutations on 2^{64} elements or 2^{512} elements respectively." However, as Portz states in the same paragraph line 2-5, "If one chooses the input size of an interconnection network according to the security constraints normally put on cryptosystems, one cannot establish the interconnection network physically any more." Therefore, Portz only describes a means of implementing in a cryptosystem a general permutation with an interconnection network such as Bennes. Where this permunation changes, it's switching can be governed by a control sequence. No where does Portz disclose or fairly suggest the claimed features of an improved DES with a variable P permutation in the f function.

Moreover, it is submitted that, even if, assuming arguendo, that the permuter 11 of Roberts is modified with the teaching of Portz of a variable permutation, the present claimed inventions would still not be taught since, as discussed above, the permuter 11 of Roberts fails to modify the internal structure of the DES algorithm and instead, after the primary DES encryption is performed and in the final step of his scheme, merely takes the 256 byte output of the 32 block encryptors and permutes the 256 bytes in conformance with a second key.

As such, it is respectfully submitted that Roberts and Portz, singly or in combination, fail to disclose or fairly suggest the features of independent claims 13, 25 and 27 concerning *in a device for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key, the combination with a modified "P" permutation in the "f" function; in a device for performing the "f" function of the Data Encryption Standard (DES), the combination with a*

modified permutation means to produce a modified permutation replacing the fixed permutation "P" of the DES; a method for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key, in combination with a modified "P" permutation in the "f" function, comprising the step of: replacing the "P" permutation in the "f" function by said modified permutation, respectively.

With regard to claim 14, it is submitted that the permutation in Roberts performs a different function and is in a different location than the modified P of the present invention, and therefore a second key controlling the permutation in Roberts fails to constitute a second cipher key to specify said modified "P" permutation, as called for in claim 14.

With regard to claim 21, it is submitted that while Portz may describe Benes networks and cites Waxman's topology, Portz is silent with regard omega networks hence the combination of Roberts and Portz does not disclose or fairly suggest the feature of claim 21 concerning said logic gates comprise an Omega network.

With regard to claim 24, it is submitted that Roberts' disclosure of the first key and second key (Col. 1, lines 54-63) which one assumes are independent, does not disclose the features of claim 24 concerning deriving a DES key and a second cipher key from a single master key.

With regard to claim 28, it is submitted that Roberts' disclosure of a second key (Col. 1, lines 54-63) does not disclose the features of claim 28 of having the modified P permutation depend upon a second cipher key.

With regard to claim 30, it is submitted that Roberts' disclosure of a second key (Col. 1, lines 54-63) does not disclose the features of claim 30 of having the modified P permutation depend upon a second cipher key which is a subset DES key and a second cipher key.

Further, with regard to dependent claims 14 – 24, 26 and 28 - 31, it is respectfully submitted that these dependent claims are allowable by virtue of their respective dependency on independent claims 13, 25 and 27.

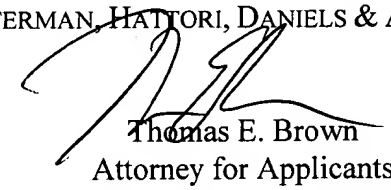
In view of the aforementioned remarks, Applicants submit that that the claims are in condition for allowance. Applicants request such action at an early date.

If the Examiner believes that this application is not now in condition for allowance, the Examiner is requested to contact Applicants' undersigned attorney to arrange for an interview to expedite the disposition of this case.

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP



Thomas E. Brown
Attorney for Applicants
Registration No. 44,450
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

TEB/jl